ABSTRACT

Described herein is a system for communicating over electrical wiring in a house or other building. Components are grouped and each group is assigned a group identifier code. Components communicates only with components of the same group, using the group identifier code. Each message includes the group identifier code, message data, and a message authentication code (MAC) that is calculated for each message. A receiving component disregards any message whose group identifier code is not the same as that of the receiving component. MACs are calculated using a shared key value and a one-way hash function. The shared key value, in turn, is taken from an ordered sequence of key values that is defined for each component group based on a counter value. To change to a new key value, one component of the group simply starts using the new key value. When a receiving component receives a message that does not authenticate using the current key value, it tries the next key value in the sequence. If the message authenticates using the next key value, the next key value is adopted as the current key value for future communications.